REMARKS

Prior to entry of this paper, Claims 1-39 were pending. Claim 1-39 were rejected. In this paper, Claims 1, 8, and 28-30 are amended. No claims are cancelled or added. Claims 1-39 are currently pending. No new matter is added by way of this amendment. For at least the following reasons, Applicants' attorneys respectfully submit that each of the presently pending claims is in condition for allowance.

Rejection of Claims

The Office Action rejected claims 1-39 under 35 U.S.C. §102(e) as being anticipated by Albert et al. (U.S. Patent Application Publication No. 2003/0177389, hereinafter "Albert"). Applicants' attorneys respectfully traverse these rejections.

Claim 1 recites, *inter alia*:

> a transceiver arranged to receive a request for access to the *resource* from a client device; and
> an *integrity management component* that is arranged to perform actions, including:
> *providing a component to the client device*;
> employing the component to gather integrity information associated with the client device at a plurality of times;
> applying a dynamic policy *for access to the resource* based, in part, on the forwarded integrity information. (Emphasis added.)

Albert does not disclose "an *integrity management component*, ..., *applying* a dynamic *policy* for access to the resource", as recited in Claim 1. Albert discloses a method "for a computer system or *device to apply a security policy* required for connection to a network" (see FIG. 3; ¶ 0025.) A security policy applied at the client device end by the client device is in contrast to a policy outside the client device (for example, at the server end) applied by the integrity management component, as recited in Claim 1. More specifically, Albert discloses that "... the integrity server 350 evaluates whether or not the client device 320 has a correct, up-to-date version of the applicable corporate security policy. ... In the event that client device 310 does not have a local copy of the most current corporate security policy ... a download of the current corporate policy may be initiated from the integrity server 350 to the client device (¶ 0072.) Therefore, Albert clearly discloses that the security policies reside on the client device. Albert further discloses that "the client security module 320 on the client device … includes … a TrueVector® engine 422, … a rules engine 424, …." (¶ 0074.) Still further, Albert discloses that "[s]ecurity rules and policy arbitration are handled by the TrueVector engine 422 and the rules engine 424." (¶ 0076.) Thus it is clear that security policies are handled at the client device by components resident on the client device, as noted above. This is in contrast to "an *integrity management component*, …, *applying* a dynamic *policy* for access to the resource", as recited in Claim 1, where the integrity management component is distinct from and external to the client device.

Furthermore, Albert does not disclose "*providing* a *component* to the client device", as recited in Claim 1. Albert discloses that a client security module 320 is already part of the client device 310 configuration, as shown in FIGURE 3, when the connection to a VPN is made through the VPN gateway 340. The security module disclosed by Albert must necessarily already be residing on the client at the time the connection is requested, because Albert discloses that the security module 320, in conjunction with the integrity server 350, control the connection of the client device 310 to the network *before* the connection is made. Hence, no such component can be provided to the client through the network before such connection is made, as recited in amended Claim 1.

Additionally, Albert discloses that "… In the event that client device 310 does not have a local copy of the most current corporate security policy … a download of the current *corporate policy* may be initiated from the integrity server 350 to the client device (emphasis added; ¶ 0072.) Albert further discloses that "a security policy is an organization's *statement defining the rules* and practices that regulate how it will provide security, …" (emphasis added; ¶ 0020.) A statement defining rules is not the same as a component that has functionality for gathering integrity information, as recited in amended Claim 1. Therefore, not only does Albert not disclose *providing* a component to the client device, but also Albert does not disclose downloading a *component*, only statements of rules.

Therefore, amended Claim 1 is submitted to be allowable for at least the reasons discussed above.

Claims 2-11 depend from Claim 1 and are submitted to be allowable for at least the reasons discussed above with respect to Claim 1.

Claim 12 recites, *inter alia*:

> receiving a request *for access to the resource* from a client device; …
> and *performing a response* based, in part, on a difference between the first integrity information and the second integrity information (emphasis added.)

Albert does not disclose "receiving a request for access to the resource, …, and performing a response …." In contrast, Albert discloses a system where a security policy is *applied at the device itself* for *connection* to the network, as opposed to performing a *response* outside the client device (for example, at the server end) distinct from the *request* for a *resource* made by the client device. Those skilled in the art will appreciate that in a client-server architecture, the requesting end (the client) and the responding end (the server) are generally distinct and communicate over a network. This is particularly true in a VPN where a network connection is used for remote access to protected resources and the client and server must be implemented as physically distinct entities. Therefore, Claim 12 is submitted to be allowable for at least the reasons discussed above.

Claims 13-17 depend from Claim 12 and are submitted to be allowable for at least the reasons discussed above with respect to Claim 12.

Claim 18 recites substantially similar features as Claim 12, in relevant parts, and is submitted to be allowable for at least the reasons discussed above with respect to Claim 12.

Claims 19-24 depend from Claim 18 and are submitted to be allowable for at least the reasons discussed above with respect to Claim 18.

Claim 25 recites substantially similar features as Claim 1, in relevant parts, and is submitted to be allowable for at least the reasons discussed above with respect to Claim 1. More specifically, Claim 25 recites, *inter alia*: "a client device configured to *request access to the resource*; and a *server*, … configured to perform actions, including: … *providing a component* to the client device; … *applying a dynamic policy* for access based, in part, on the forwarded integrity information." (Emphasis added.) As noted above with respect to Claim 1, Albert does not disclose, teach, or suggest requesting access to a resource, *providing a component* to the client device, and *applying* the dynamic policy *by the server* (as opposed to by the client device itself.) Therefore, Claim 25 is submitted to be allowable for at least the reasons discussed above.

Claims 26 and 27 depend from Claim 25 and are submitted to be allowable for at least the reasons discussed above with respect to Claim 25.

Claim 28 has been amended to further clarify claim language without narrowing the scope of the claim. Claims 28 and 31 recite substantially similar features as Claim 1, and Claims 12 and 25, in relevant parts, and are submitted to be allowable for at least the reasons discussed above with respect to Claim 1, and Claims 12 and25.

Claims 29 and 30, and Claims 32-39 depend from Claims 28 and 31, respectively, and are submitted to be allowable for at least the reasons discussed above with respect to Claims 28 and 31.

CONCLUSION

It is respectfully submitted that each of the presently pending claims (Claims 1-39) is in condition for allowance and notification to that effect is requested. Examiner is invited to contact the Applicants' representative at the below-listed telephone number if it is believed that the prosecution of this application may be assisted thereby. Although only certain arguments regarding patentability are set forth herein, there may be other arguments and reasons why the claimed invention is patentable. Applicant reserves the right to raise these arguments in the future.

Dated: July 18, 2008

Respectfully submitted,

By
Jamie L. Wiegand
Registration No.: 52,361
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770
(206) 262-8915
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant